



DoD PKI Automatic Key Recovery

**(520) 538-8133 or Coml. 866 738-3222,
netcom-9sc.om-iacacpki.helpdesk@mail.mil
Fort Huachuca, AZ 85613-5300
4 December 2015**





The Problem:



One problem in the past with the DoD PKI infrastructure was the inability to recover Common Access Card (CAC) private encryption keys and certificates that were either expired or revoked. This becomes necessary when a CAC is lost and its certificates are revoked or when a CAC and the certificates it contains simply expires and is surrendered to DEERS/RAPIDS before the user's encrypted emails have been decrypted.

An Auto Key Recovery capability has been fielded by DISA to permit holders of new CACs to retrieve encryption keys/certificates from previous cards to permit decryption of old email.



The Solution:



Steps to Recover CAC Private Email Encryption Keys

The following slides identify steps to recover private encryption keys, escrowed by DISA, from CACs that do not have the “Auto Key Recovery” functionality.



URL for Key Recovery

<https://ara-1.c3pki.chamb.disa.mil/ara/Key>

Or

<https://ara-2.c3pki.den.disa.mil/ara/Key>

Or

<https://ara-3.csd.disa.mil/ara/Key>

Or

<https://ara-4.csd.disa.mil/ara/Key>

These are the Automatic Key Recovery URLs. They can only be accessed from the .mil network (NIPRNet). TLS 1.1 and 1.2 MUST be enabled

Note: The URL addresses shown above are case sensitive.

When you go to this link, you must identify yourself with PKI credentials. Use ONLY your identity certificate!



At this time open the
URL

<https://ara-1.c3pki.chamb.disa.mil/ara/Key>

Or

<https://ara-2.c3pki.den.disa.mil/ara/Key>

Or

<https://ara-3.csd.disa.mil/ara/Key>

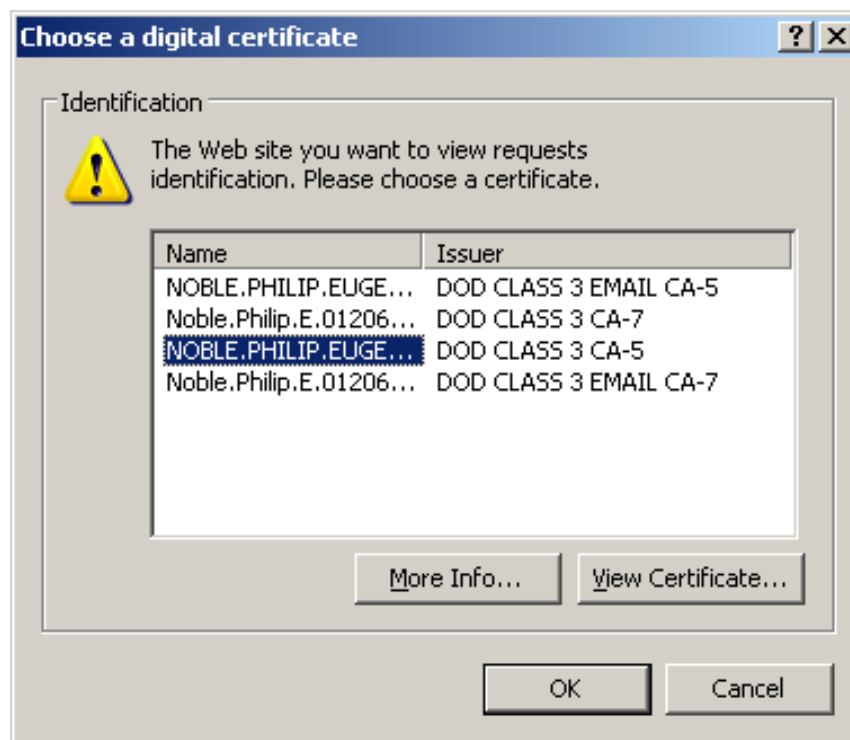
Or

<https://ara-4.csd.disa.mil/ara/Key>

Note: You may have to go to all four URLs listed and download all keys available that are four years old or newer to get the correct key to decrypt emails. If that fails, look at the instructions listed on slides 28 and 29.



Choose Your CAC Identity Certificate



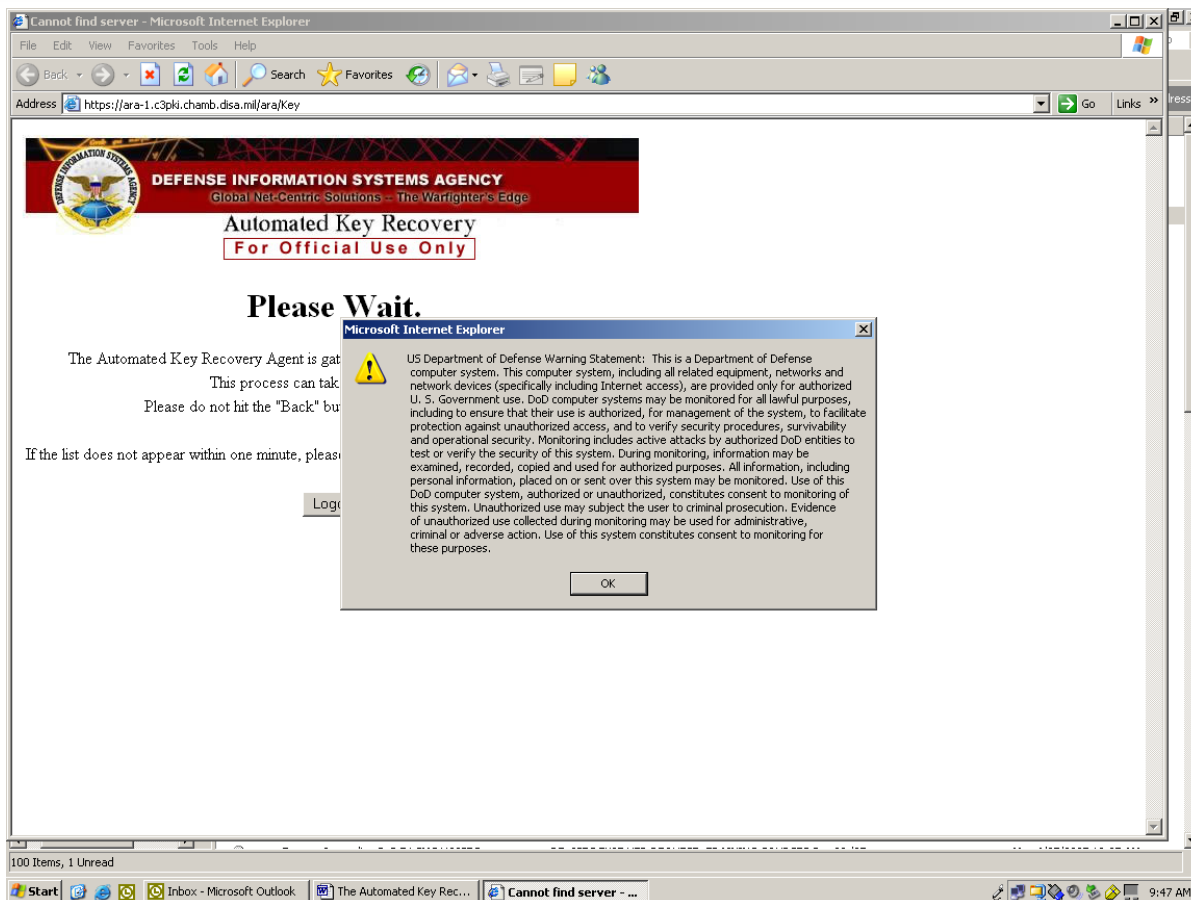
You will be prompted to identify yourself.

Highlight your Identification Certificate from your CAC. Select it by clicking “OK”.

Note: Do NOT choose any that contain the word “EMAIL” from the Issuer column.



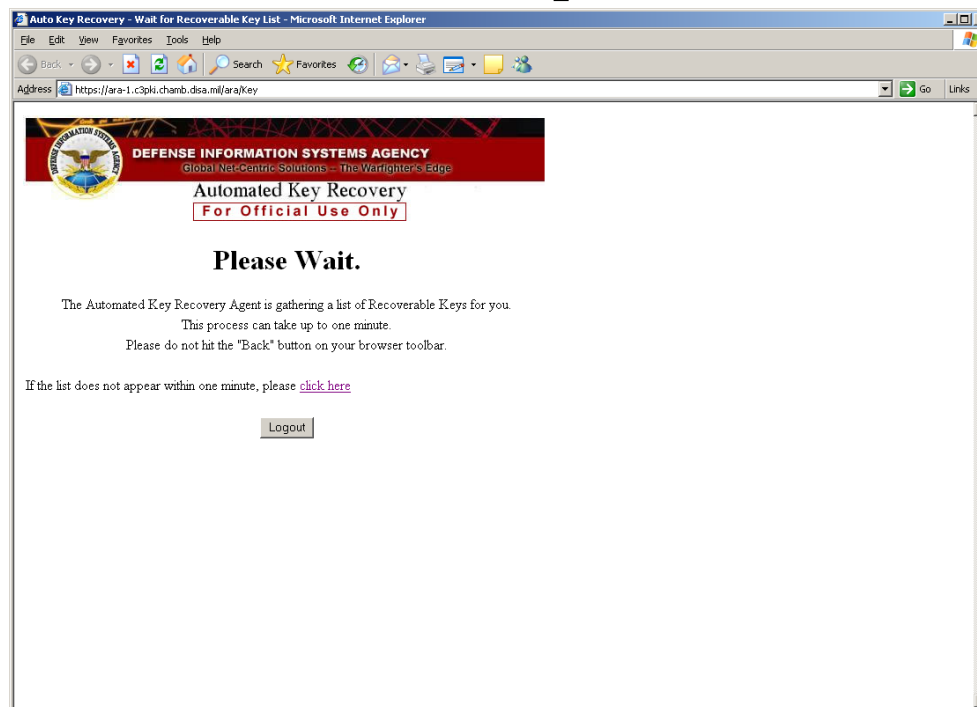
Warning Banner



Dismiss the warning by clicking “OK”.



Processing Your Request



The Automated Key Recovery Agent will compile a list of Recoverable Keys. Should recovery fail or if the key is unable to be downloaded automatically, contact the Army Key Recovery Agent by sending a signed email to: usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil requesting recovery of your private email encryption Key. **Please Wait...**



Key Selection



Auto Key Recovery - Recoverable Key List - Microsoft Internet Explorer

File Edit View Favorites Tools Help

Back Forward Stop Reload Search Favorites

Address <https://ara-1.c3pi.chamb.dsa.mil/ara/Key?value=96287> Go Links

 **DEFENSE INFORMATION SYSTEMS AGENCY**
Global Net-Centric Solutions - The Warfighter's Edge

Automated Key Recovery
For Official Use Only

The following Encryption Keys can be recovered:

Common Name:	NOBLE PHILIP EUGENE.1184204718	Recover
Organization Affiliation:	USA	
Not Before:	2002-04-29 00:00:00 GMT	
Not After:	2005-04-28 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-4	
Serial #	0x05DCF3	
Revocation Status:	REVOKED	

Common Name:	NOBLE PHILIP EUGENE.1184204718	Recover
Organization Affiliation:	USA	
Not Before:	2004-01-28 00:00:00 GMT	
Not After:	2007-01-27 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-5	
Serial #	0x0DD98B	

Common Name:	NOBLE PHILIP EUGENE.1184204718	Recover
Organization Affiliation:	USA	
Not Before:	2003-08-18 00:00:00 GMT	
Not After:	2004-02-02 00:00:00 GMT	
Email:	philip.noble@us.army.mil	
Issuer:	DOD CLASS 3 EMAIL CA-5	
Serial #	0x0DD98B	

Browse through the list and locate the appropriate key you want to recover. When located, click the adjacent associated "Recover" button.

U.S. Army Materiel
Command |

Communications-Electronics
Command



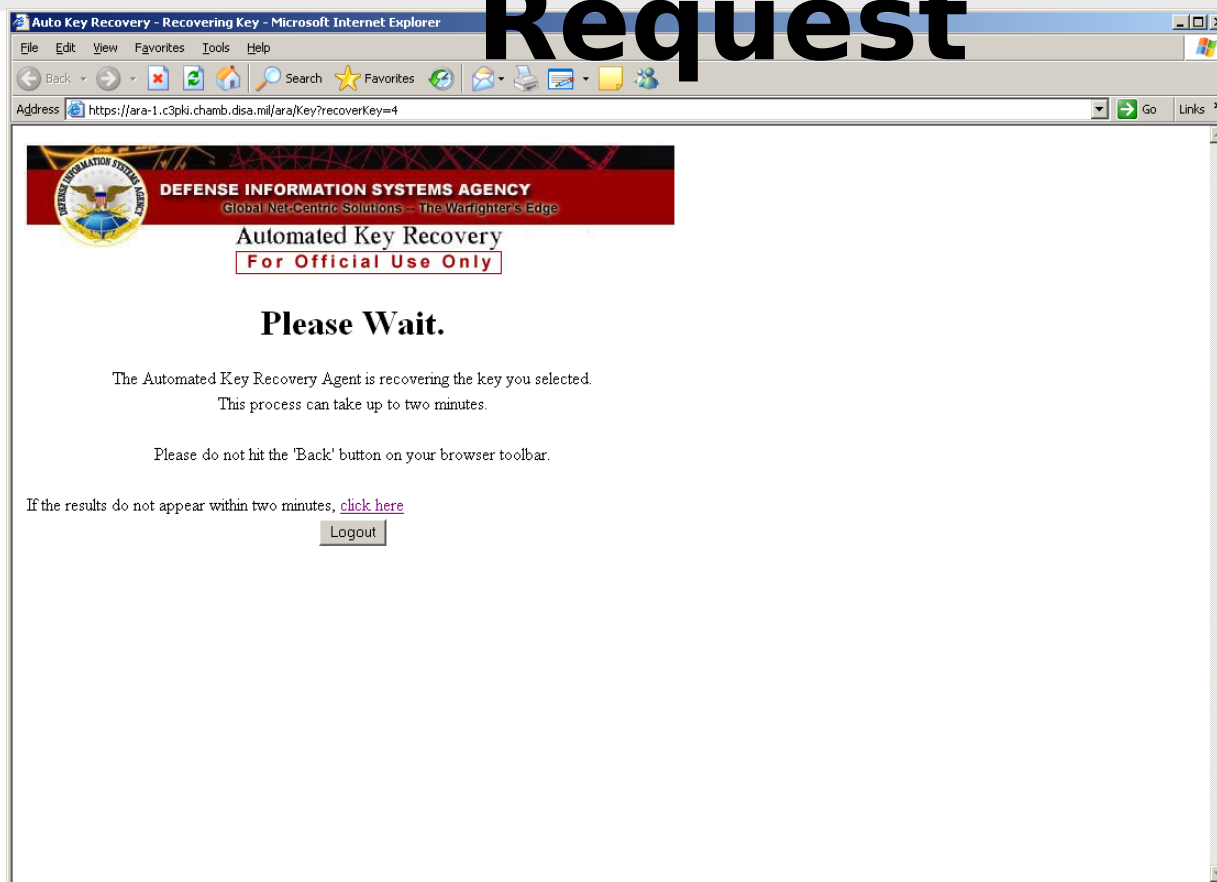
Acknowledgement of DoD Subscriber



Select “OK”.



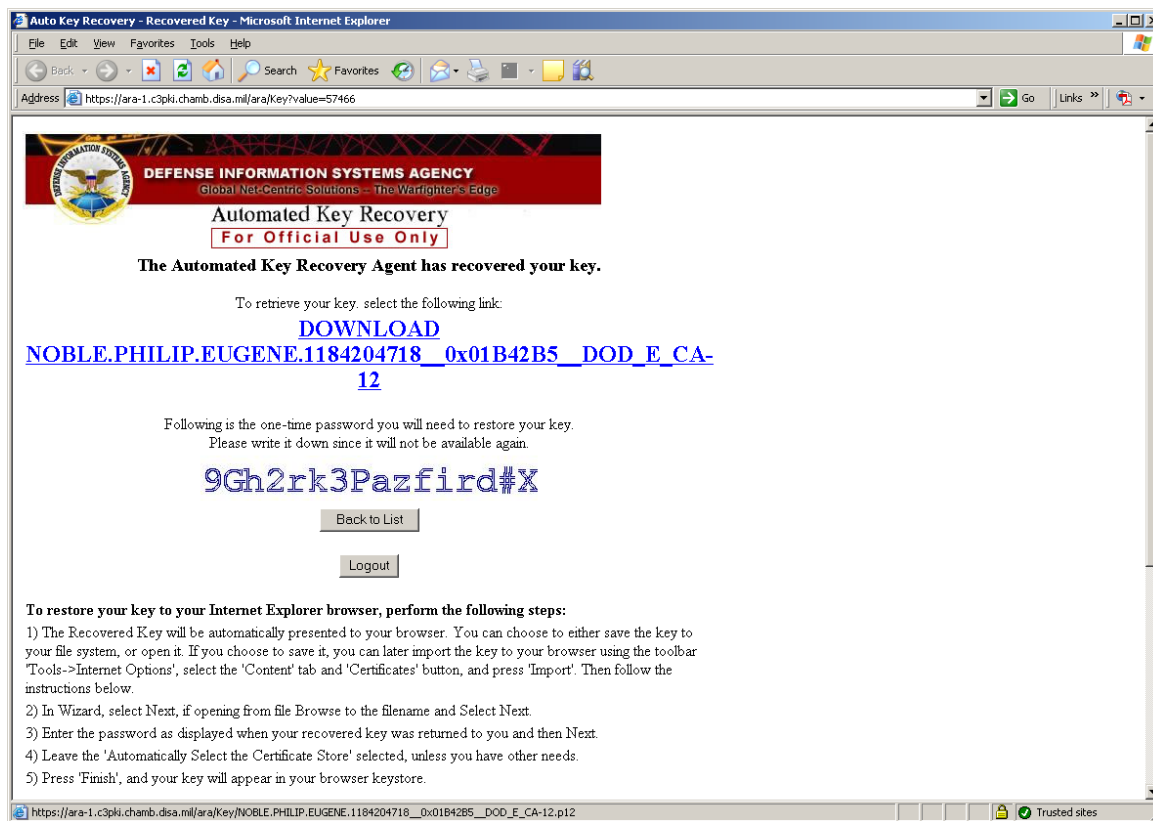
Processing Request



The Automated Key Recovery Agent is processing your request. Please Wait...



One-time PIN



This is your one-time PIN to access your Private Encryption Key if it's saved as a separate file.

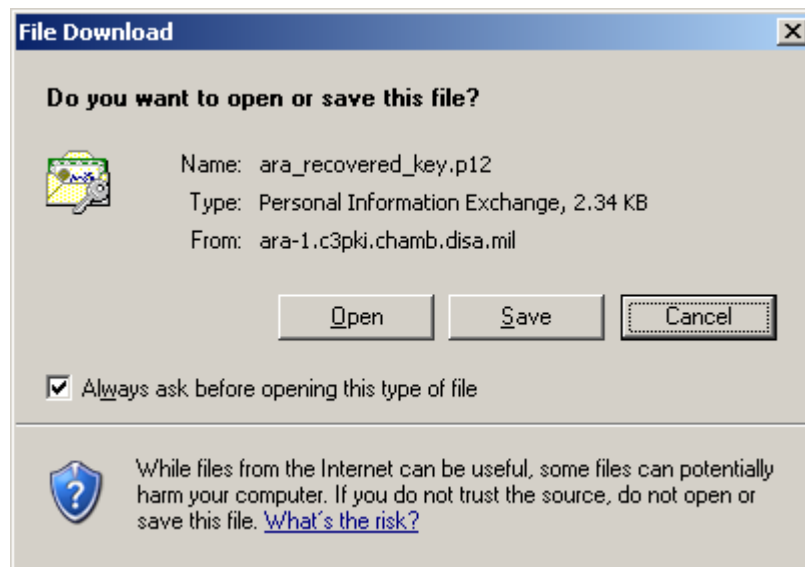
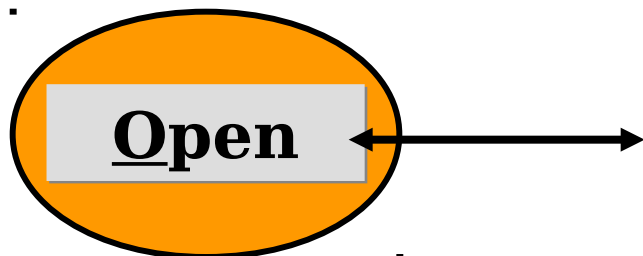
Also, you will find instructions for both Netscape and Internet Explorer web browsers.

U.S. Army Materiel
Command |

Communications-Electronics
Command



Installing the Certificate



You will be given the opportunity to install the certificate, click “Open”.



Installing the Certificate (Cont'd)



Click “Next”.



Installing the Certificate (Cont'd)



Certificate Import Wizard

File to Import
Specify the file you want to import.

File name:

Note: More than one certificate can be stored in a single file in the following formats:

- Personal Information Exchange- PKCS #12 (.PFX, .P12)
- Cryptographic Message Syntax Standard- PKCS #7 Certificates (.P7B)
- Microsoft Serialized Certificate Store (.SST)

Click “Next”.



Installing the Certificate (Cont'd)



Certificate Import Wizard

Password

To maintain security, the private key was protected with a password.

Type the password for the private key.

Password:

☒ Enable strong private key protection. You will be prompted every time the private key is used by an application if you enable this option.

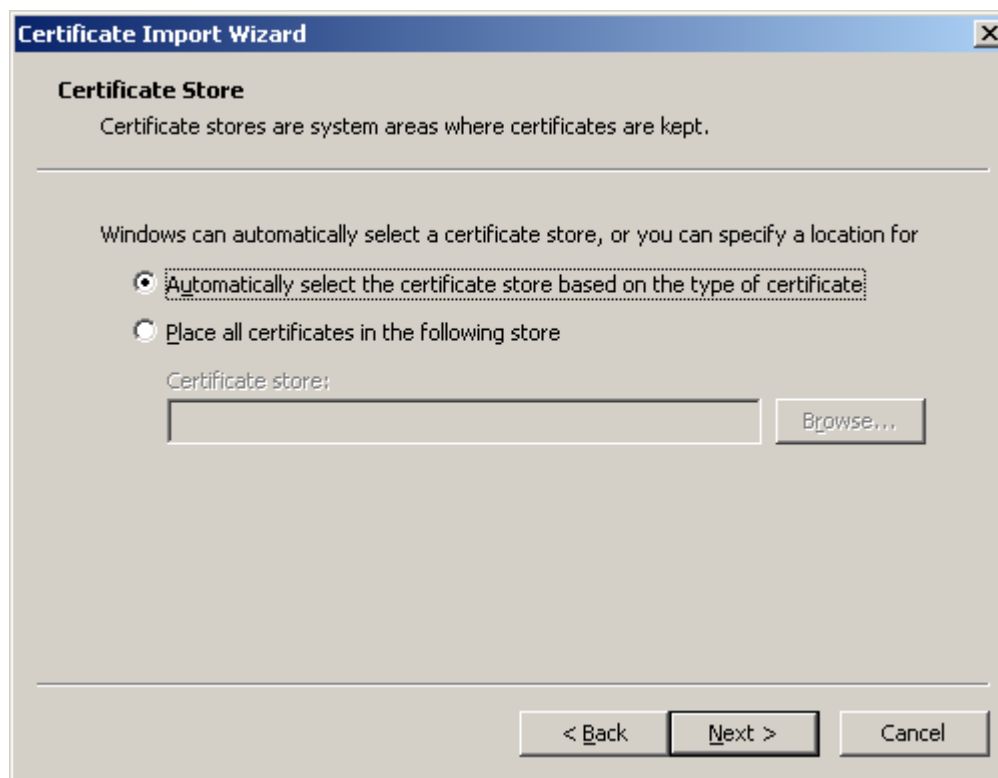
☐ Mark this key as exportable. This will allow you to back up or transport your keys at a later time.

< Back Next > Cancel

Leave the check blocks unchecked, enter your Password, and click “Next”.



Installing the Certificate (Cont'd)



Ensure that “*Automatically select the certificate store based on the type of certificate*” is selected (as shown above) and click “Next**”.**



Installing the Certificate (Cont'd)



Click “Finish”.



Installing the Certificate (Cont'd)



Click "OK"



Installing the Certificate (Cont'd)



Click "OK".



Medium Security is Not a Choice



If Medium Security is blocked and High Security is default, refer to:
<http://blogs.technet.com/b/pki/archive/2009/06/17/what-is-a-strong-key-protection-in-windows.aspx>

Use gpedit.msc:

- Local computer policy
 - Windows settings
 - Security settings
 - Local policies
 - Security options

Temporarily set - **System Cryptography: Force Strong Protection for User Keys Stored on the Computer to User Input is Not Required When New Keys are Stored and Used**

After the key is imported, change the setting to - **User Must Enter a Password Each Time They Use a Key**



Importing The Recovered Key



From MEPCOM:

During the process of importing the certificate, the user receives the following Password Error no matter what password is entered : **‘The password supplied does not meet the minimum complexity requirements’**. Almost simultaneously the following error appears: **‘Windows has encountered a critical problem and will restart automatically in one minute’**. The error condition has also been encountered during the process of attempting to recover email certificates. In many cases, local security policies may not allow the use of **‘Medium Security’** from the previous page.



Importing The Recovered Key



Solution: The enpasflt.dll is in use and must be unloaded to correct the issue. Log into the computer using an account with administrative rights to complete the following:

- Click Start | Type **regedit** | **Press Enter**
- Navigate to HKLM\System\CurrentControlSet\Control\LSA | Navigate to Notification Packages in the right pane
- Remove the **enpasflt entry** | **Ensure that the scecli entry remains**
- Restart the computer

Note: After the certificates have been loaded or recovered, you will need to re-install the EnPasFlt

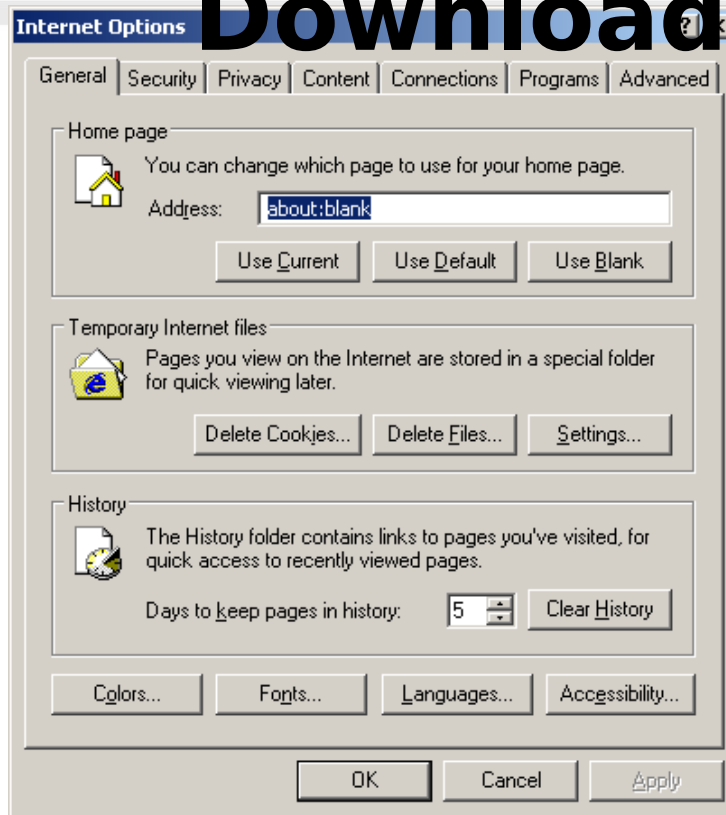
- Navigate to C:\Windows\AGMSupport\EnPasFlt
- Double Click **Installer.exe**

Note: This install is silent and applies immediately

- Open **regedit**
- Navigate to HKLM\System\CurrentControlSet\Control\LSA\Notification Packages
- Ensure that the **enpasflt entry is present**
- Close **regedit**



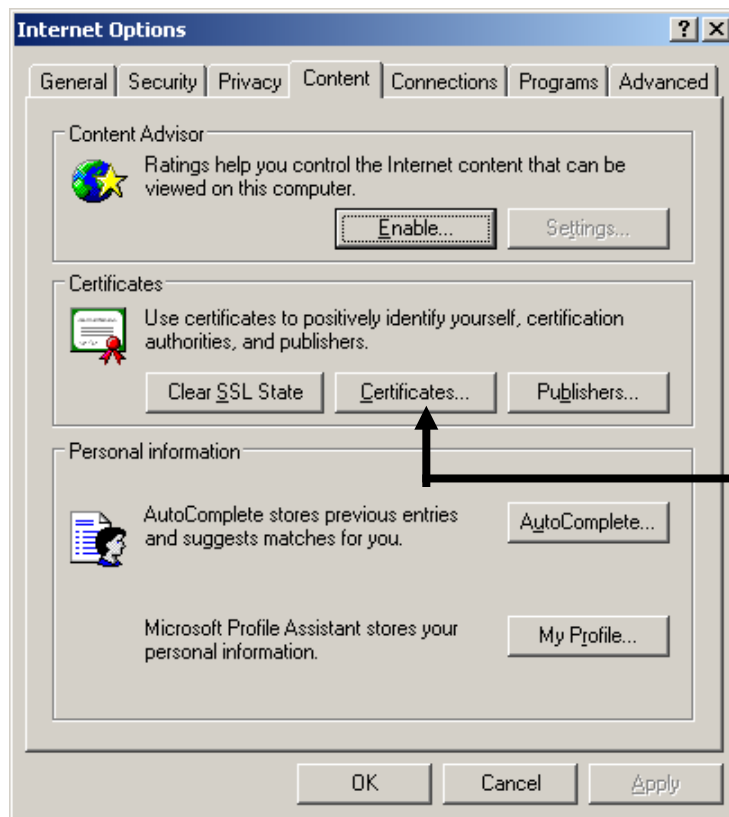
Verifying the Download



You can verify the successful download of your recovered Private Encryption Key by performing the following; Launch Internet Explorer, select “Tools” from the menu, and then “Internet Options”.



Verifying the Download (Cont'd)

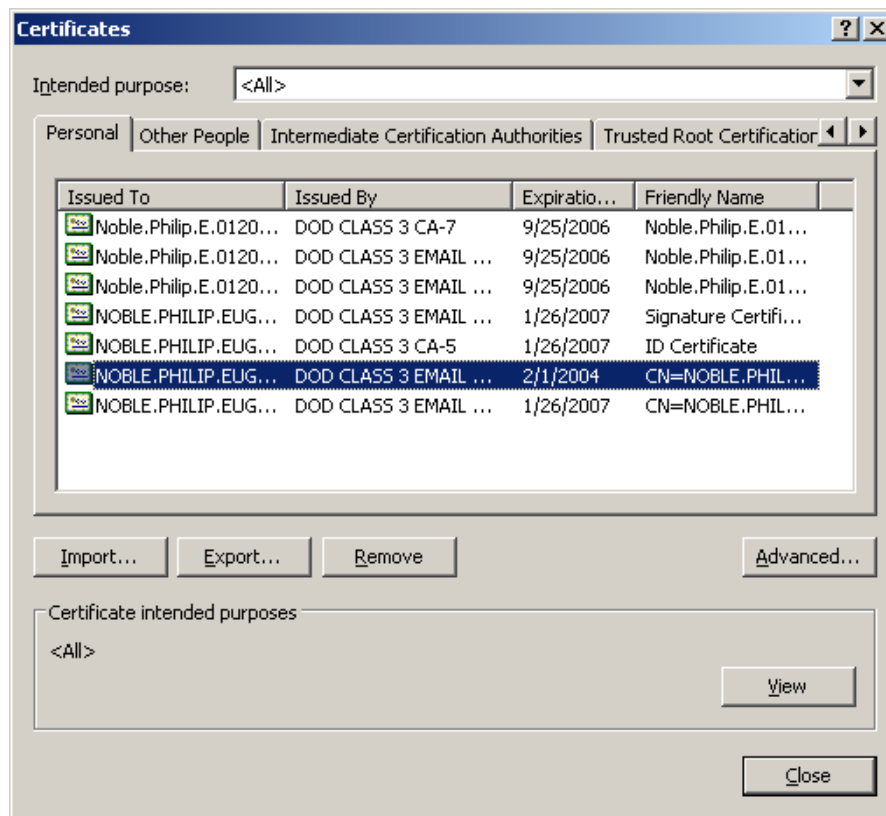


**Certificate
S...**

**Click the “Content” tab. Now, click
“Certificates”.**



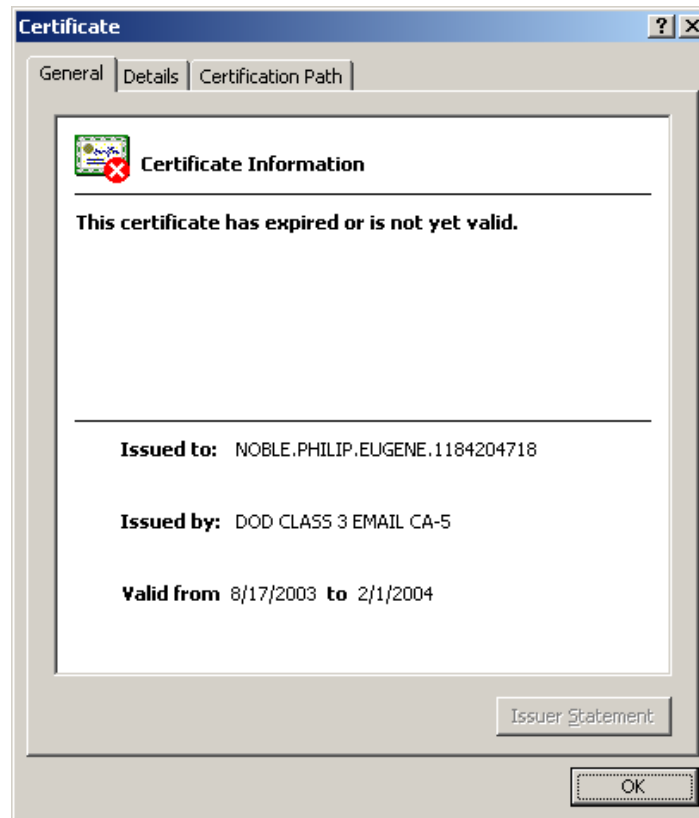
Verifying the Download (Cont'd)



Select the “Personal” tab and you will see a list of your currently registered certificates, including the recovered new key certificate.



Verifying the Download (Cont'd)



Double-click on the certificate and you can view the specifics of your recovered key (or other current keys) as illustrated above.



Success



**Close the open window, you may now use
the recovered key to access your
encrypted email.**

Last Step: If you chose to save the recovered key to a file instead of directly installing the key, delete the saved .P12 file from your computer as this is a security vulnerability and will be detected in a Q-tip Scan. Disregard if you did not save the key to a file

Should recovery fail, contact the Army Key Recovery Agent by sending a signed email to:
usarmy.pentagon.hqda-cio-g-6.mbx.army-registration-authority@mail.mil

Send the digitally signed email requesting recovery of old PKI encryption certificates and provide the following:

1. Your name and by your name your 10 digit EDIP (ex. Doe.John.1234567890)
2. The CA certificate was issued on (ex. CA20)
3. The serial number (ex. 0x12fA3).
4. Also please provide the exact reason for having to recover your keys
5. The key(s) you need recovered



Other Services



Navy Key Recovery Agent

<https://infosec.navy.mil/PKI/>
NCMS_NAFW_NAVY_RA@navy.mil
Phone: 800-304-4636
DSN 588-4286

USMC RA Operations Helpdesk

Email: raoperations@mcnosc.usmc.mil
Phone: 703-432-0394

Air Force PKI Help Desk

Phone: 1-210-925-2521
Email: afpki.ra@lackland.af.mil
<https://afpki.lackland.af.mil/html/lracontacts.asp> (this site is accessible from .mil domains only)
Additional Air Force PKI support is available from the Air Force PKI help desk:
https://afpki.lackland.af.mil/html/help_desk.asp

DISA PKI Help Desk Oklahoma City, OK Support:

E-Mail: disa.tinker.eis.mbx.okc-service-desk@mail.mil
1-844-347-2457, then select options 1, 5 and 4 in that order



Recovery Notification Example



A user has attempted to recover a key using the Automated Key Recovery Agent. The ID Certificate used for Authentication was: CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0B5643, Issuer: DOD CLASS 3 CA-5. The key that was recovered was: CN=NOBLE.PHILIP.EUGENE.1184204718,OU=USA,OU=PKI,OU=DOD,O=U.S. GOVERNMENT,C=US, Serial: 0x0C8747, Issuer: DOD CLASS 3 EMAIL CA-3.

If you did not perform this operation, please contact your local key recovery agent and ask that they check the logs for the key recovery at Fri Jul 01 16:48:12 GMT 2005 with session ID 1.c3pki.chamb.disa.mil-23f%3A42c57335%3A68e46e9395fb9727.

**You will receive an email from
PKI_ChambersburgProcessingElement@csd.disa.mil
with a subject "ALERT! Key Recovery Attempt
Using Automated Key Recovery Agent" similar to
the above Recovery Notification example notifying
you of your recovery action.**



POC for Additional Information



Philip E. Noble
USAISEC
Information Assurance and Security
Engineering Directorate (IASSED)
DSN 879-7608
CML 520-538-7608
FAX DSN 879-8709 CML 520-538-
8709 philip.e.noble.civ@mail.mil
philip.noble@us.army.smil.mil
philip.noble@us.army.smil.mil